UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/607,678	06/26/2003	Vincent J. Zimmer	42P16421	8063

7590 06/14/2007

R. Alan Burnett
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
COVINGTON, JONATHAN H	
ART UNIT	**PAPER NUMBER**
2109	
MAIL DATE	**DELIVERY MODE**
06/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/607,678	ZIMMER ET AL.	
	Examiner	Art Unit	
	Jonathan Covington	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 June 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 - 30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the following communication: Non-provisional application filed 26 June 2003.

2. Claims 1 – 30 are pending in the case. Claims 1, 15, 18, 21, 25 and 28 are the independent claims.

Double Patenting

3. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101, which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

4. Claims 1 – 30 are provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims 1 – 30 of copending Application No. 10/462,996. This is a provisional double-patenting rejection since the conflicting claims have not in fact been patented.

5. Claims 1 – 30 are directed to the same invention as that of claims 1 – 30 of commonly assigned 10/462,996. The issue of priority under 35 U.S.C. 102(g) and possibly 35 U.S.C. 102(f) of this single invention must be resolved.

Since the U.S. Patent and Trademark Office normally will not institute an interference between applications or a patent and an application of common ownership (see MPEP Chapter 2300), the assignee is required to state which entity is the prior inventor of the conflicting subject matter. A terminal disclaimer has no effect in this situation since the basis for refusing more than one patent is priority of invention under 35 U.S.C. 102(f) or (g) and not an extension of monopoly.

Failure to comply with this requirement will result in a holding of abandonment of this application.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. **Claims 1 – 10, 13 – 19, 21 – 25, 27, 28 and 30 are rejected under 35 U.S.C. 103(a) as being obvious over IEEE's Port-Based Network Access Control protocol (802.1X-2001) in view of the Intelligent Platform Management Interface (IPMI) Specification (version 1.5, revision 1.1, February 20, 2002).**

As to independent claim 1, and dependent claims 9, 10, 13 and 14, IEEE's Port-Based Network Access Control protocol teaches:

Claim 1 – a method comprising … authenticating a network port ("a means of authenticating and authorizing devices attached to a LAN port," abstract) hosted by an authenticator system ("An entity that provides an authentication service to an authenticator," p. 5, definition 3.1.2. Examiner notes that definition 3.1.6 on the same page defines a 'system' as "A device that is attached to a LAN by one or more ports. Examples of systems include … servers …," which would render the 'authenticator system' of claim 1 and 'authentication server' of definition 3.1.2 functionally equivalent) to which the supplicant system ("An entity at one end of a point-to-point LAN segment

that is being authenticated by an authenticator attached to the other end of that link," p. 5, definition 3.1.5) is linked ("The point of attachment to the LAN can be provided by any physical or logical Port that can provide a one-to-one connection to a Supplicant System," p. 8, last paragraph) via execution of the port authentication firmware instructions on the supplicant system ("The Port Access Entity (PAE) operates the Algorithms and Protocols associated with the authetication mechanisms ... In the Supplicant role, the PAE is responsible for responding to requests from an Authenticator for information that will establish its credentials," p.8, first and second paragraphs).

Claim 9 – the method of claim 1, wherein port authentication is performed using the EAPOL (extensible authentication protocol over local area network) protocol ("The Authenticator makes use of the uncontrolled Port to communicate ..., using EAPOL protocol exchanges," p. 11, and figure 8-4, p. 29).

Claim 10 – the method of claim 1, wherein the port is authenticated using an access/challenge scheme (figure 8-4, p. 29).

Claim 13 – the method of claim 1, wherein a determination of whether a port is authenticated is made by an authentication server that is linked in communication with the authenticator system (figures 8-1 and 8-2, p. 28).

Claim 14 – the method of claim 1, further comprising providing a callable interface [by] which a port authentication process can be invoked ("sending an EAP-Request/Identity frame ... is typically how an Authenticator PAE will begin the authentication exchange," p. 25, second paragraph under heading 8.4.2.1. This is the 'call' to which the interface responds).

As to independent claims 15, 18, 21, 25 and 28, and dependent claim 19, IEEE's Port-Based Network Access Control protocol teaches:

Claim 15 – a method comprising:

executing instructions comprising port authentication code … in a supplicant system to perform port authentication of an authenticator system port to which the supplicant system is linked in communication (IEEE teaches this as discussed in regard to claim 1 above).

Claim 18 – a method comprising:

retrieving authentication credentials pertaining to a supplicant system ("the Authenticator … is responsible for communication with the Supplicant, and for submitting the information received from the Supplicant to a suitable Authentication Server in order for the credentials to be checked and for the consequent authorization state to be determined," p. 8, third paragraph under heading 6.2) … and

authenticating a network port to which the supplicant system is connected via use of the authentication credentials ("authentication service … determines, from the credentials provided by the supplicant, whether the supplicant is authorized," p. 5, definition 3.1.2).

Claim 19 – the method of claim 18, wherein the operating system is compliant with the IEEE 802.1x port-based network access control standard and authenticates the network port via an 802.1x authentication protocol ("the Extensible Authentication

Protocol ... is a general protocol that supports multiple authentication mechanisms," first paragraph under heading 8.4.1).

Claim 21 – a machine-readable medium on which firmware instructions are stored, which when executed by a supplicant system perform operations including:

authenticating a network port hosted by an authenticator system to which the supplicant system is linked (IEEE teaches this as discussed in regard to claim 1 above).

Claim 25 – a supplicant system comprising:

a processor;

a network interface, coupled to the processor (this describes an ordinary computer with a network card); and

firmware instructions ... that when executed on the processor perform operations including:

authenticating a network port hosted by an authenticator system to which the supplicant system is linked in communication via the network interface (IEEE teaches this as discussed in regard to claim 1 above).

Claim 28 – a supplicant system comprising:

a network interface (See claim 25 above) ... and

machine-executable instructions stored on the supplicant system, which when executed ... perform operations including:

authenticating a network port hosted by an authenticator system to which the supplicant system is linked in communication via the network interface (IEEE teaches this as discussed in regard to claim 1 above).

As to independent claims 1, 15, 18, 25 and 28, and dependent claims 2 – 8, 16, 17, 22 – 24, 27 and 30, IEEE's Port-Based Network Access Control protocol does not appear explicitly to disclose the following, whereas the IPMI specification teaches:

Claim 1 – loading port authentication firmware instructions in a supplicant system ("The IPMI specifications include support for storing and accessing ... non-volatile ... imformation," p. 12, first paragraph under heading 1.6.11; see also figure 1-2 on p. 9. Whether in dedicated memory or not, authentication cannot take place without first loading the instructions in the supplicant system to do so).

Claim 15 – a method comprising:

executing instructions ...via a baseboard management controller (BMC) in a supplicant system ("The management architecture can be implemented by centralizing the most common functions into a 'central' management controller in the system. This controller is often called the *Baseboard Management Controller,* or BMC," p. 23, under heading 3).

Claim 18 – a method comprising:

retrieving authentication credentials pertaining to a supplicant system during a pre-boot phase of the supplicant system ("IPMI ... can provide platform management in a 'pre-boot' or 'OS-absent' environment," p. 15, first paragraph under heading 1.6.20);

passing the authentication credentials to an operating system running on the supplicant system (This step is inherent in the process of handing off data from the base

management controller to the system management software, or "SMS ... that runs under the OS," p. 85, first paragraph under heading 10.1. Such an exchange takes place through the Server Management Interface Chip, "[t]he SMIC interface ... specified for transferring IPMI messages between the system management software and the system's primary management controller (BMC)," p. 85, first paragraph under heading 10) during an operating system runtime phase (IPMI teaches this as discussed in regard to claim 4 below).

Claim 25 – a supplicant system comprising:

... a flash device coupled to the processor (flash is mentioned four times in the specification, each time as a place data may be stored – p. 162, third paragraph; p. 311, second paragraph; and p. 325, first and third paragraphs), having firmware instructions stored therein (IPMI teaches this as discussed in regard to claim 1 above).

Claim 28 – a supplicant system comprising:

a baseboard management controller (BMC) ("The management architecture can be implemented by centralizing the most common functions into a 'central' management controller in the system. This controller is often called the *Baseboard Management Controller,* or BMC," p. 23, under heading 3, emphasis in original);

a network interface, coupled to the baseboard management controller ("LAN Interface," p. 27, third definition); and

machine-executable instructions stored on the supplicant system, which when executed on the BMC perform operations (See above. As a controller, the BMC by definition performs operations based on the instructions loaded onto it).

Claim 2 – that the network port of claim 1 is authenticated during a pre-boot phase ("IPMI ... can provide platform management in a 'pre-boot' or 'OS-absent' environment," p. 15, first paragraph under heading 1.6.20).

Claim 3 – that in addition to claim 2, an operating system image is loaded into the supplicant system over a network that is accessed via the network port that is authenticated (network boot is referred to in Table 36-3, p. 362).

Claim 4 – that the network port of claim 1 is authenticated during an operating system (OS)-runtime phase ("The key characteristic of Intelligent Platform Management is that inventory, monitoring, logging, and recovery control functions are available independent of the main processors, BIOS, and operating system," p. 8, first paragraph under heading 1.6.1. 'Monitoring' and 'logging' 'independent of the operating system' is taken to mean that ports may be checked or authenticated without any interaction with the operating system, all the while running simultaneous with the operating system; or in the case of the operating system not running at all, that the ports may be checked or authenticated in the absence of the operating system).

Claim 5 – that in addition to claim 4, network port authentication is performed by executing the port authentication firmware using a hidden mode that is transparent to an operating system running on the supplicant system during the OS-runtime phase (As in claim 4 above, "monitoring [and] logging functions are available independent of the ...

operating system," p. 8, first heading under heading 1.6.1. Examiner interprets 'transparent to an operating system' as isolated from the operating system, and thus to the user. As these functions are carried out without the recognition of software or user, they are hidden.).

Claim 6 – that in addition to claim 5, the hidden execution mode is a system management mode (SMM) ("Upon entry into SMM, the processor state is saved and a memory configuration is entered where the SMI Handler has full access to system memory and I/O space. This allows the SMI Handler to implement its management functions in an OS-independent manner," p.19, second paragraph under heading 1.9. This fits the description quoted in claim 4).

Claim 7 – that in addition to claim 6, the firmware instructions are embodied as one or more SMM handlers ("The SMI Handler is typically a routine that is loaded and initialized into a protected area of memory by the BIOS," p.19, second paragraph. The interrupts effectively call the handlers, which accomplish the functions intended by their assertion, making them functionally 'instructions.' IPMI teaches this as discussed in regard to claim 6 above).

Claim 8 – that the following steps are to be added to claim 7:

asserting one of an SMI (system management interrupt) or PMI (Processor Management Interrupt) on a processor of the supplicant ("When [an SMI is] asserted, it switches the processors into 'System Management Mode' (SMM)," p. 19, second paragraph under heading 1.9) on a periodic basis (IEEE, "regular reauthentication of the Supplicant," p. 6, item (c) (6) under heading 5.1);

dispatching said one or more SMM handlers to handle the SMI or PMI event (IPMI teaches this as discussed in regard to claim 7 above) via operations including

determining [whether] a network port needs to be authenticated (IPMI teaches this as discussed in regard to claim 4 above); and in response thereto,

authenticating the network port (IPMI teaches this as discussed in regard to claim 1 above).

Claim 16 – the method of claim 15, wherein the port authentication code is stored in a non-volatile storage device coupled to the BMC (See figure 1-2, p. 9. Each portion of the figure marked 'SEEPROM' represents a Serial Electrically Erasable Programmable Read-Only Memory, which is a non-volitile storage device. The first four letters of this acronym are spelled out on p. 12, under heading 1.6.10; the last three are common knowledge in the art), the method further comprising loading the port authentication code into the BMC for execution ("At the heart of the IPMI architecture is a *microcontroller* called the ... BMC," p. 9, first paragraph under heading 1.6.3, emphasis added. By definition, a microcontroller must load its instructions before executing them).

Claim 17 – the method of claim 15, wherein the port authentication is performed during an operating system runtime phase (IPMI teaches this as discussed in regard to claim 4 above).

Claim 22 – the machine-readable medium of claim 21, wherein the media comprises a firmware storage device (IPMI teaches this as discussed in regard to claim 1 above).

Claim 23 – the machine-readable medium of claim 21, wherein firmware instructions comprise at least one system management mode (SMM) handler (IPMI teaches this as discussed in regard to claim 7 above) that is executed by a processor of the supplicant system while operating in SMM.

Claim 24 – the machine-readable medium of claim 21, wherein the network port is authenticated during a pre-boot phase of the supplicant system (IPMI teaches this as discussed in regard to claim 2 above).

Claim 27 – the supplicant system of claim 25, wherein the processor includes a hidden execution mode and the network port is authenticated during an operating system runtime phase via execution of firmware instructions under the hidden execution mode (IPMI teaches this as discussed in regard to claim 5 above).

Claim 30 – the supplicant system of claim 28, wherein the machine-executable instructions are stored in one of the BMCs or a non-volatile storage device coupled to that BMC (IPMI teaches this as discussed in regard to claim 1 above).

IEEE's Port-Based Network Access Control protocol and the IPMI specification are analogous art because they are from the same field of endeavor, that of network-access control.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of IEEE and the IPMI specification, to modify the authenticaton scheme of IEEE's 802.1x to include storage of the authentication instructions in firmware, to execute these instructions during a pre-boot phase, and further to load an operating-system image over the network connection so

authenticated.

The motivation for doing so would have been to take advantage of the behind-the-scenes feature (IPMI grants "information access out-of-band or under 'system down' conditions," p. 13, first paragraph) of IPMI to streamline network authentication. On p. 362, in table 36-3, an "Out-of-band Access Password" is mentioned as an indication that system administrators may put a measure of confidence in IPMI's design. The authors of the specification themselves suggest that "[a]s out-of-band management using RMCP [Remote Management Control Protocol, p. 107] *becomes more popular*, network controller vendors may offer controllers with the ability to directly respond to ARP [Address Resolution Protocol, p. 116, first paragraph under heading 12.7] Requests when the system is powered down or sleeping," p. 118, fourth bullet, emphasis added. Enterprises have a vested interest in keeping up with current technology.

Therefore, it would have been obvious to combine IEEE's Port-Based Network Access Control protocol with the IPMI specification to obtain the invention as specified in the instant claims.

8. **Claims 11 and 20 are rejected under 35 U.S.C. 103(a) as being obvious over IEEE's Port-Based Network Access Control protocol (802.1X-2001) in view of the Intelligent Platform Management Interface (IPMI) Specification (version 1.5, revision 1.1, February 20, 2002), and further in view of PPP EAP TLS Authentication Protocol (EAP-TLS, RFC 2716, The Internet Society, October 1999). The teachings of IEEE and IPMI are listed above.**

As to dependent claims 11 and 20, IEEE's Port-Based Network Access Control protocol and the Intelligent Platform Management Interface Specification do not appear explicitly to disclose the following, whereas EAP-TLS teaches:

Claim 11 – the method of claim 10, wherein the access/challenge scheme employs a Transport Layer Security (TLS) challenge response in which authentication is determined based on credentials provided by the supplicant system ("the peer sending and EAP-Response packet ... The data field of that packet will encapsulate one or more TLS records," p. 2, third paragraph under heading 3.1. The supplicant's credentials are taken to be such a record. Examiner notes also that 'peer' and 'supplicant' are synonymous in the art.)

Claim 20 – the method of claim 19, wherein the network port is authenticated using a Transport Layer Security (TLS) challenge response in which authentication is determined based on the authentication credentials (EAP-TLS teaches this as discussed in regard to claim 11 above).

IEEE's Port-Based Network Access Control protocol, the IPMI specification, and EAP-TLS are analogous art because they are from the same field of endeavor, that of network-access control.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of IEEE, IPMI and the Internet Society, to modify the authenticaton scheme of IEEE's 802.1x, with the trusted subsystem of IPMI, to include the steps of EAP-TLS.

The suggestion for doing so would have been that 802.1X leaves the

particulars of which authentication protocol to use up to the network administrator.

Therefore, it would have been obvious to combine IEEE's Port-Based Network Access Control protocol, together with IPMI's out-of-band baseboard management, with EAP-TLS to obtain the invention as specified in the instant claims.

9. **Claim 12 is rejected under 35 U.S.C. 103(a) as being obvious over IEEE's Port-Based Network Access Control protocol (802.1X-2001) in view of the Intelligent Platform Management Interface (IPMI) Specification (version 1.5, revision 1.1, February 20, 2002), also in view of the PPP EAP TLS Authentication Protocol (EAP-TLS, RFC 2716, The Internet Society, October 1999), and further in view of of the Trusted Computing Platform Alliance's (TCPA) Main Specification (version 1.1b, February 22, 2002). The teachings of IEEE, IPMI and EAP-TLS are listed above.**

As to dependent claim 12, IEEE's Port-Based Network Access Control protocol, the Intelligent Platform Management Interface Specification, and the PPP EAP TLS Authentication Protocol do not appear explicitly to disclose the following, whereas TCPA's specification teaches:

Claim 12 – the method of claim 11, wherein the TLS challenge response employs credentials stored in a Trusted Platform Module (TPM) ("The TCG Architechture requires credentials to prove various pieces of information," p.282, second paragraph under heading 9.5; also figure on p. 83 under heading 4.32), and wherein the

method further comprises retrieving the credentials from the TPM ("an organization vouches for the TPM ... checks the ... credentials of the TPM," etc., p.6, fourth paragraph under heading 2.3.2).

IEEE's Port-Based Network Access Control protocol, the IPMI specification, EAP-TLS, and TCPA's specification are analogous art because they are from the same field of endeavor, that of network-access control.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of IEEE, IPMI, the Internet Society, and the TCPA, to modify the authenticaton scheme of IEEE's 802.1x, the details of EAP-TLS, with the trusted subsystem of IPMI, to include storage of the credentials in a trusted platform module.

The motivation for doing so would have been to strengthen security, as the TPM vigorously protects its identity and that of the platform of which it is a part.

Therefore, it would have been obvious to combine IEEE's Port-Based Network Access Control protocol using the specifics of EAP-TLS, together with IPMI's out-of-band baseboard management, with TCPA's specification to obtain the invention as specified in the instant claims.

10. **Claims 26 and 29 are rejected under 35 U.S.C. 103(a) as being obvious over IEEE's Port-Based Network Access Control protocol (802.1X-2001) in view of the Intelligent Platform Management Interface (IPMI) Specification (version 1.5,**

revision 1.1, February 20, 2002), and further in view of of the Trusted Computing Platform Alliance's (TCPA) Main Specification (version 1.1b, February 22, 2002). The teachings of IEEE and IPMI are listed above.

As to dependent claims 26 and 29, IEEE's Port-Based Network Access Control protocol and the Intelligent Platform Management Interface Specification do not appear explicitly to disclose the following, whereas TCPA's specification teaches:

Claim 26 – the supplicant system of claim 25, further comprising a trusted platform module (TPM) coupled to the processor ("This specification defines a trusted *Subsytem* that is an integral part of each platform," p. 1, second paragraph of the Forward [sic], emphasis in original. This implies that the TPM has a secondary role to the system's main processor, and as an integral part, is connected thereto), to store authentication credentials employed for authenticating the network port (IPMI teaches this as discussed in regard to claim 12 above).

Claim 29 – the supplicant system of claim 28, further comprising a trusted platform module coupled to the BMC ("The Subsystem itself will have basic functions that maintain privacy, yet support the identity and authentication of entities ..." p. 1, second paragraph of the Forward [sic]. The TPM thus works hand-in-hand with the BMC), to store authentication credentials employed for authenticating the network port (IPMI teaches this as discussed in regard to claim 12 above).

IEEE's Port-Based Network Access Control protocol, the IPMI specification, and TCPA's specification are analogous art because they are from the same field of

endeavor, that of network-access control.

At the time of the invention, it would have been obvious to one of ordinary skill in the art, having the teachings of IEEE, IPMI, and the TCPA, to modify the authenticaton scheme of IEEE's 802.1x with a trusted subsystem of IPMI, to include storage of the credentials in a trusted platform module.

The motivation for doing so would have been to strengthen security, as the TPM vigorously protects its identity and that of the platform of which it is a part.

Therefore, it would have been obvious to combine IEEE's Port-Based Network Access Control protocol, together with IPMI's out-of-band baseboard management, with TCPA's specification to obtain the invention as specified in the instant claims.

11. The following prior art is made of record and not relied upon, yet is considered pertinent to applicant's disclosure:

Gage et al.	US 6,035,405
Nagel, Paul.	US 6,173,405
Stoltz et al.	US 6,615,264
Giles et al.	US 6,968,420
Brannock, Kirk D.	US 7,103,641
Neuman et al.	US 2002/0162026
See et al.	US 2003/0021283
Hunter et al.	US 2006/0161784

Blunk & Vollbrecht . "PPP Extensible Authentication Protocol (EAP)," RFC 2284, the Internet Society, March 1998

Dobbelsteijn, Erik. "What about 802.1X? An overview of possibilities for safe access to fixed and wireless networks," SURFnet slide presentation, www.surfnet.nl/innovatie/wlan/802.1Xen.pdf, Amsterdam, 29 October 2002

PC21100 (SAFEKEEPER) LPC-Based TCPA-Compliant Security Controller, National Semiconductor product brief, revision 1.0, http://ortodoxism.ro/datasheets/nationalsemiconductor/PC21100.pdf, February 2002

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan Covington whose telephone number is 571-270-3023. The examiner can normally be reached on 7:30 - 5:00 M-F, Alternate Fri off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Del Sole can be reached on 571-272-1130. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

JOSEPH DEL SOLE
SUPERVISORY PATENT EXAMINER
6/11/07

***